такая, что либо $H_{i-1}$ нормальна в $H_i$, либо $|H_i : H_{i-1}|$ – простое число для любого $i = 1, \ldots, n$.

**Теорема 1.** Пусть группа $G$ имеет три сверхразрешимые подгруппы $A$, $B$ и $C$, чьи индексы попарно взаимно просты в $G$. Тогда:

1. Если $A$, $B$ и $C$ попарно взаимно sn-перестановочны, то $G$ сверхразрешима.

2. Если $A$, $B$ и $C$ K-**P**-субнормальны в $G$, то $G$ сверхразрешима.

## Литература

1 Ballester-Bolinches, A. Products of Finite Groups / A. Ballester-Bolinches, R. Esteban-Romero, M. Asaad. – Berlin-New York: Walter de Gruyter. – 2010. – 334 p.

2 Васильев, А. Ф. О K-**P**-субнормальных подгруппах конечных групп / А. Ф. Васильев, Т. И. Васильева, В. Н. Тютянов // Мат. заметки. – 2014. – Т. 95, № 4. – С. 517–528.

**В. В. Парченкова, Ю. Я. Романовский**
(ГрГУ им. Я. Купалы, Гродно)

## КИНЕМАТИКА ЗАМЕЧАТЕЛЬНЫХ ТОЧЕК ТРЕУГОЛЬНИКА

Практическая значимость данного исследования заключается в том, что кинематические модели могут использовать школьники и взрослые при решении реальных ситуаций; учителя, как при проведении уроков по математике, так и на факультативных курсах. Данное исследование будет полезным для разработки электронных графических изображений, а так же в спортивной деятельности.

Целью исследования является: рассмотрение следа замечательных точек треугольника, оставленных после перемещения вершины по различным прямым, предварительно зафиксировав остальные.

Похожие исследования проводились Кирилюк Л.В. при рассмотрении ортоцентров треугольника [1]. В данной работе исследованы следы замечательных точек треугольника оставленных после движения вершины по трем различным прямым: 1) по прямой перпендикулярной к основанию; 2) по прямой пересекающей основание треугольника, но не перпендикулярной к ней; 3) по прямой параллельной основанию.

В результате было установлено, что данные точки не хаотично разбросаны на плоскости, а описывают некоторые линии. Построены кинематические модели центров описанных окружностей и ортоцентров для вышеуказанных случаев.

Данная работа будет интересна для изучения не только школьникам и педагогам, а так же студентам учреждений высшего образования.

**Литература**

1 Кирилюк, Л. В. Живые треугольники / Л. В. Кирилюк // Альфа. – 1997. – № 1. – С. 11–16.

**В. Е. Писпанен, А. С. Поздняков, А. Ф. Васильев**
(ГГУ им. Ф. Скорины, Гомель)

## ТЕОРИЯ ГРУПП В КРИПТОГРАФИИ

Криптография – наука о методах обеспечения конфиденциальности, целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта), а также невозможности отказа от авторства [1].

Криптография требует, чтобы были заданы множества целых чисел и операции, определенные для них. Комбинация множеств и операций, которые могут быть применены к элементам множества, называются алгебраической структурой.

Клод Шеннон предложил рассматривать блочные шифры как наиболее перспективное средство обеспечения конфиденциальности сообщений в системах секретной связи. Он построил свою первую модель секретной системы с помощью алгебры шифров, введя понятия их суммы и произведения [2].

Современные симметрично-ключевые блочные шифры выполняют операции с n-битовыми словами. Понимание этих шифров требуют знания разделов современной алгебры, называемых алгебраическими структурами. Одной из таких структур являются группы.

Группа (G) – набор элементов с бинарной операцией «*» обладает следующими свойствами: замкнутость, ассоциативность, коммутативность, существование нейтрального элемента и существование инверсии.

Хотя группа включает единственный оператор, свойства, присущие каждой операции, позволяют использование пары операций, если они – инверсии друг друга. Если оператор – сложение, то группа поддерживает и сложение, и вычитание как аддитивно инверсные операции. Это